AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1-21 (canceled)

22 (currently amended) A content reproduction system for use with a plurality of contents, the content reproduction system comprising:

a recording medium;

a content distribution apparatus; and

a reproduction apparatus,

wherein the recording medium is operable to store, in association with each other, (i) identification information for identifying a plurality of contents that can be acquired, (ii) a master key that is common to the~~a~~ plurality of contents, and (iii) ~~and~~ rule information that indicates a use rule that is common to the plurality of contents,

wherein the content distribution apparatus includes:

a storage unit for storing a plurality of encrypted contents and a plurality of encrypted content keys associated with the plurality of encrypted contents, the plurality of encrypted contents being generated by encrypting each of the plurality of contents by using one or more of a plurality of content keys, the one or more of the plurality of content keys being uniquely assigned to the each of the plurality of contents, the plurality of encrypted content keys being generated by encrypting the plurality of content keys, respectively, using the master key;

a transmitting unit operable to transmit, to the reproduction apparatus, a content list including content IDs which respectively indicate all contents held by the content distribution apparatus; and

a distribution unit operable to distribute an encrypted content requested by the reproduction apparatus and an encrypted content key associated with the encrypted content to the reproduction apparatus in response to a request from the reproduction apparatus, without using

the recording medium as an intermediary,

wherein the reproduction apparatus includes:

a reading unit operable to read out the master key and the rule information from the recording medium;

a display unit operable to read out the identification information from the recording medium, to select, based on the read out identification information, one or more acquirable content IDs from among the content IDs included in the content list received from the content distribution apparatus, and to display an acquirable content list composed of the selected one or more acquirable content IDs;

a receiving unit operable to receive an acquirable content ID of the selected one or more acquirable content IDs from a user with the use of the displayed acquirable content list;

an acquiring unit operable to request an encrypted content from the content distribution apparatus, the encrypted content corresponding to the received acquirable content ID, and to acquire the requested encrypted content and an encrypted content key associated with the encrypted content, without using the recording medium;

a decrypting unit operable to determine if the acquired encrypted content is permitted to be used, based on the use rule indicated by the rule information and, if the acquired encrypted content is permitted to be used, to acquire the content key by decrypting the encrypted content key using the master key, and to generate a decrypted content using the acquired content key; and

a reproducing unit operable to reproduce the decrypted content, and

wherein the recording medium is insertable into the reproduction apparatus and removable from the reproduction apparatus.

23 (previously presented) The content reproduction system of Claim 22,

wherein the recording medium stores the master key as an encrypted master key generated by encrypting the master key using a device key uniquely assigned to the reproduction apparatus, and

wherein the reading unit acquires the master key by decrypting the encrypted master key using the device key uniquely assigned to the reproduction apparatus.

24 (currently amended) A reproduction apparatus for use in a content reproduction system with a content distribution apparatus and a recording medium which stores, in association with each other, (i) identification information for identifying a plurality of contents that can be acquired, (ii) a master key that is common to the~~a~~ plurality of contents, and (iii) ~~and~~ rule information that indicates a use rule that is common to the plurality of contents,

wherein the content distribution apparatus is for storing a plurality of encrypted contents and a plurality of encrypted content keys associated with the plurality of encrypted contents, the plurality of encrypted contents being generated by encrypting each of the plurality of contents by using one or more of a plurality of content keys, the one or more of the plurality of content keys being uniquely assigned to the each of the plurality of contents, the plurality of encrypted content keys being generated by encrypting the plurality of content keys, respectively, using the master key, and

wherein the content distribution apparatus is operable to transmit, to the reproduction apparatus, a content list including content IDs which respectively indicate all contents held by the content distribution apparatus, and to distribute an encrypted content requested by the reproduction apparatus and an encrypted content key associated with the encrypted content to the reproduction apparatus in response to a request from the reproduction apparatus, without using the recording medium as an intermediary,

the reproduction apparatus comprising:

a reading unit operable to read out the master key and the rule information from the recording medium;

a display unit operable to read out the identification information from the recording medium, to select, based on the read out identification information, one or more acquirable content IDs from among the content IDs included in the content list received from the content distribution apparatus, and to an acquirable content list composed of the selected one or

more acquirable content IDs;

a receiving unit operable to receive an acquirable content ID of the selected one or more acquirable content IDs from a user with the use of the displayed acquirable content list;

an acquiring unit operable to request an encrypted content from the content distribution apparatus, the encrypted content corresponding to the received acquirable content ID, and to acquire the requested encrypted content and an encrypted content key associated with the encrypted content, without using the recording medium as an intermediary;

a decrypting unit operable to determine if the acquired encrypted content is permitted to be used based on the use rule indicated by the rule information, and if the acquired encrypted content is permitted to be used, operable to acquire the content key by decrypting the encrypted content key using the master key and to generate a decrypted content by decrypting the acquired encrypted content key using the acquired content key; and

a reproducing unit operable to reproduce the decrypted content, and

wherein the reproduction apparatus is configured so that the recording medium is insertable into the reproduction apparatus and removable from the reproduction apparatus.

25 (previously presented) The reproduction apparatus of Claim 24,

wherein the recording medium stores the master key as an encrypted master key that is generated by encrypting the master key based on a device key uniquely assigned to the reproduction apparatus, and

wherein the reading unit acquires the master key by decrypting the encrypted master key using a device key uniquely assigned to the reproduction apparatus.

26 (previously presented) The reproduction apparatus of Claim 25,

wherein the recording medium stores another encrypted master key that is different from the encrypted master key, the another encrypted master key being generated by encrypting another master key, the another master key being different from the master key, based on the device key, and

wherein the reading unit further acquires the another master key by decrypting the another encrypted master key using the device key.

27 (previously presented) The reproduction apparatus of Claim 24,

wherein the recording medium stores the master key as an encrypted master key set that is generated by encrypting a master key set based on a device key uniquely assigned to the reproduction apparatus, the master key set including the master key and another master key that is different from the master key, and

wherein the reading unit acquires the master key set by decrypting the encrypted master key set using the device key uniquely assigned to the reproduction apparatus and acquires the master key from the acquired master key set.

28 (previously presented) The reproduction apparatus of Claim 24,

wherein the rule information further indicates a use period of the content,

wherein the acquiring unit further includes:

an acquisition information receiving sub-unit operable to receive acquisition information that indicates either rental, which means that the content is acquired for rent, or purchase which means that the content is acquired for purchase; and

an acquisition information storage sub-unit operable to store therein the received acquisition information in association with the encrypted content and the encrypted content key, and

wherein the decrypting unit is further operable to determine (i) if the received acquisition information indicates purchase or (ii) if the acquisition information indicates rental and a requested use period for the content is within the use period indicated by the rule information, and operable to decrypt the encrypted content based on a result of the determination.

29 (previously presented) The reproduction apparatus of Claim 28,

wherein the decrypting unit is further operable to calculate a period between (i)

acquisition of the encrypted content and (ii) the encrypted content key and reception of the reproduction instruction, and operable to determine if the calculated period is within the use period of the content.

30 (previously presented) The reproduction apparatus of Claim 28,

wherein the recording medium further stores usable content information that indicates a condition for using the content, the usable content information being different from the rule information, and

wherein the acquiring unit is further operable to determine if the condition for using the content is satisfied, and operable to acquire the encrypted content and the encrypted content key from the content distribution apparatus if the condition for using the content is satisfied.

31 (previously presented) The reproduction apparatus of Claim 30,

wherein the content distribution apparatus is further operable to distribute the encrypted content and the encrypted content key to the reproduction apparatus without a content distribution request from the reproduction apparatus, and

wherein the acquiring unit is further operable to determine if the received encrypted content and encrypted content key satisfy the condition indicated by the usable content information, and operable to hold the received encrypted content and encrypted content key only if the received encrypted content and encrypted content key satisfy the condition indicated by the usable content information.

32 (previously presented) The reproduction apparatus of Claim 24,

wherein the use rule indicates a value that has been prepaid as a payment for using the encrypted content, and

wherein the decrypting unit is further operable to determine whether or not the encrypted content is permitted to be used in exchange for consuming the value indicated by the use rule, and operable to consume the value indicated by the use rule and decrypt the encrypted content if

the encrypted content is permitted to be used in exchange for consuming the value indicated by the use rule.

33 (previously presented) The reproduction apparatus of Claim 24,

wherein the use rule indicates a time period in which the encrypted content is permitted to be decrypted, and

wherein the decrypting unit is further operable to determine if a current time is within the time period indicated by the use rule, and to decrypt the encrypted content if the current time is within the time period.

34 (currently amended) A content distribution apparatus for use in a content reproduction system with a reproduction apparatus and a removable recording medium which stores, in association with each other, (i) identification information for identifying a plurality of contents that can be acquired, (ii) a master key that is common to the~~a~~ plurality of contents, and (iii) ~~and~~ rule information that indicates a use rule that is common to the plurality of contents, the content distribution apparatus comprising:

a storage unit for storing a plurality of encrypted contents and a plurality of associated encrypted content keys associated with the plurality of encrypted contents, the plurality of encrypted contents being generated by encrypting each of the plurality of contents by using one or more of a plurality of content keys, the one or more of the plurality of content keys being uniquely assigned to the each of the plurality of contents, the plurality of encrypted content keys being generated by encrypting the plurality of content keys, respectively, using the master key;

a transmitting unit operable to transmit, to the reproduction apparatus, a content list including content IDs which respectively indicate al contents held by the content distribution apparatus; and

a distribution unit operable to distribute an encrypted content requested by the reproduction apparatus and an encrypted content key associated with the encrypted content to the reproduction apparatus in response to a request from the reproduction apparatus, without using

the recording medium as an intermediary,

wherein the content list is used by the reproduction apparatus to select, based on the identification information, one or more acquirable content IDs from amount the content IDs included in the content list, to receive an acquirable content ID of the selected one or more acquirable content IDs from a user, and to request a content corresponding to the received acquirable content ID.

35 (previously presented) The content distribution apparatus of Claim 34 further comprising:

a master key storage unit for storing a plurality of master keys and for storing a state for each master key of the plurality of master keys;

a state changing unit operable to set a state of a master key that is not permitted to be used among the plurality of master keys to an unusable state; and

a content key encrypting unit operable to generate an encrypted content key using a master key that is permitted to be used among the plurality of master keys.

36 (currently amended) A reproduction method for reproducing content with a reproduction apparatus used with a content distribution apparatus and a recording medium which stores, in association with each other, (i) identification information for identifying a plurality of contents that can be acquired, (ii) a master key that is common to the~~a~~ plurality of contents, and (iii) ~~and~~ rule information that indicates a use rule that is common to the plurality of contents,

wherein the recording medium is insertable into the reproduction apparatus and removable from the reproduction apparatus,

wherein the content distribution apparatus is for storing a plurality of encrypted contents and a plurality of encrypted content keys associated with the plurality of encrypted contents, the plurality of encrypted contents being generated by encrypting each of the plurality of contents by using one or more of a plurality of content keys, the one or more of the plurality of content keys being uniquely assigned to the each of the plurality of contents, the plurality of encrypted content

keys being generated by encrypting the plurality of content keys, respectively, using the master key, and

wherein the content distribution apparatus is operable to transmit, to the reproduction apparatus, a content list including content IDs which respectively indicate all contents held by the content distribution apparatus, and to distribute an encrypted content and an encrypted content key associated with the encrypted content to the reproduction apparatus in response to a request from the reproduction apparatus, without using the recording medium as an intermediary,

the reproduction method comprising the steps of:

reading out from the recording medium the master key that is common to the plurality of contents and the rule information that indicates the use rule that is common to the plurality of contents;

reading out the identification information from the recording medium;

selecting, based on the read out identification information, one or more acquirable content IDs from among the content IDs included in the content list received from the content distribution apparatus, displaying an acquirable content list composed of the selected one or more acquirable content IDs, and receiving an acquirable content ID from a user with the use of the displayed acquirable content list;

requesting one encrypted content from the content distribution apparatus, the encrypted content corresponding to the received acquirable content ID, and acquiring the requested encrypted content and an encrypted content key associated with the requested encrypted content, without using the recording medium as an intermediary;

determining if the acquired encrypted content is permitted to be used, based on the use rule, and if the acquired encrypted content is permitted to be used, acquiring the content key by decrypting the encrypted content key using the master key and generating a decrypted content by decrypting the acquired encrypted content key using the acquired content key; and

reproducing the decrypted content.

37 (currently amended) A computer-readable storage medium storing a reproduction

program for use in a computer and with a content distribution apparatus and a recording medium which stores, in association with each other, (i) identification information for identifying a plurality of contents that can be acquired, (ii) a master key that is common to thea plurality of contents, and (iii) and rule information that indicates a use rule that is common to the plurality of contents,

wherein the recording medium is insertable into the computer and removable from the computer,

wherein the content distribution apparatus is for storing a plurality of encrypted contents and a plurality of encrypted content keys associated with the plurality of encrypted contents, the plurality of encrypted contents being generated by encrypting each of the plurality of contents by using one or more of a plurality of content, the one or more of the plurality of content keys being uniquely assigned to the each of the plurality of contents, the plurality of encrypted content keys being generated by encrypting the plurality of content keys, respectively, using the master key, and

wherein the content distribution apparatus is operable to transmit, to the computer, a content list including content IDs which respectively indicate all contents held by the content distribution apparatus, and to distribute an encrypted content requested by the computer and an encrypted content key associated with the encrypted content to the computerreproduction apparatus in response to a request from the computerreproduction apparatus, without using the recording medium as an intermediary,

the reproduction program being for causing the computer to perform the steps of:

reading out from the recording medium the master key that is common to the plurality of contents and the rule information that indicates the use rule that is common to the plurality of contents;

reading out the identification information from the recording medium;

selecting, based on the read out identification information, one or more acquirable content IDs from among the content IDs included in the content list received from the content distribution apparatus, displaying an acquirable content list composed of the selected one or more

acquirable content IDs, and receiving an acquirable content ID from a user with use of the displayed acquirable content list;

requesting one encrypted content from the content distribution apparatus, the encrypted content corresponding to the received acquirable content id, and acquiring the requested encrypted content and an encrypted content key associated with the requested encrypted content, without using the recording medium;

determining if the acquired encrypted content is permitted to be used, based on the use rule, and if the acquired encrypted content is permitted to be used, acquiring the content key by decrypting the encrypted content key using the master key and generating a decrypted content by decrypting the acquired encrypted content key using the acquired content key; and

reproducing the decrypted content.